Appendix O
for “Rules of procedure for
the Board of Atrium Ljungberg AB”

Personal Data Policy
Atrium Ljungberg AB

(Resolved at the Board meeting on 16/05/2023)

Purpose

Atrium Ljungberg AB and its subsidiaries (which are jointly referred as the ‘Group’ in this document) processes and manages personal data in accordance with the General Data Protection Regulation, and adopts policies and guidelines for processing and protecting personal data.

Responsibility

Atrium Ljungberg’s Board of Directors adopts the company’s Personal Data Policy.

Atrium Ljungberg’s Personal Data Policy is to be revised regularly and adopted by the Board at least once a year. The Personal Data Protection Officer is the document owner and responsible for this policy.

Organisation

Personal Data Protection Officer

Atrium Ljungberg does not need to have a General Data Protection Officer as defined by the General Data Protection Regulation, as we are not a company that processes a substantial amount of personal data. However, Atrium Ljungberg must have a Personal Data Protection Officer, who is responsible for ensuring that personal data is processed correctly and that there is adequate protection for this data. The Personal Data Protection Officer must always be asked if there are any questions that relate to the processing and protection of personal data.

Personal data processing requirements

All personal data that we collect must be correct, relevant and up-to-date. There must be a clear purpose, reasons and legal grounds for processing this data.

Retention period

A maximum retention period must be set for all personal data.

Information

Every time we collect new personal data or update existing personal data, we must provide information to the data subjects about who the personal data controller is, the entire purpose of collecting the data and the legal basis for processing the data.

As far as internal staff and agency workers are concerned, each line manager is responsible for informing them about the processing of personal data for their employment or recruitment.

Sensitive personal data

In addition to the statutory requirements, sensitive personal data may only be collected to comply with the company’s obligations or to exercise its rights as an employer.

Impact analysis

A risk analysis must be performed before introducing any measures that involve new or revised processing of personal data that could risk the privacy of the data subject. This analysis must also propose suitable routines and measures to address any risks that have been identified. The initiator of the change is responsible for initiating the risk analysis and must contact the Personal Data Protection Officer if they need any support. Agreements that include the processing of personal data must always be checked and approved by the Personal Data Protection Officer.

Deletion

Any personal data that does not satisfy the requirements in this policy or that has reached its maximum retention period must be deleted.

Protection

Personal data must be processed and stored in such a way that it is protected from unauthorised access, alteration or deletion.

Corrections

Checks and routines must be in place to ensure that any inaccurate or misleading personal data that are identified or become known are managed in such a way that they are immediately deleted or corrected without delay.

Rights of data subjects

Personal data must always be processed in a way that safeguards the rights of the data subjects in accordance with the General Data Protection Regulation.

Incident management

A documented process must be in place for reporting and managing personal data incidents.

Record

There must be a central record of all personal data processing activities within the group.

Suppliersand partners

The company must have personal data processing agreements with all suppliers that process or store personal data on behalf of the company, setting out requirements to provide adequate protection of this personal data.

Periodic checks

Processes must be in place for reporting and monitoring compliance with the Personal Data Policy and its associated guidelines.

Regular monitoring, documentation and reporting of the level of compliance throughout the Group must be carried out as an integral part of day-to-day operations. The Personal Data Protection Officer is responsible for ensuring that monitoring and reporting are carried out at least once a year.

Reporting must include, as a minimum:

- Follow-up of the effectiveness of checks, including assessment data.
- Reporting of incidents/deviations from the policy, along with a description.
- Action(s) with a description, what will be achieved by the action(s) and when the action(s) will be taken to address the incident/deviation
- Follow-up of outstanding actions and completion reporting